5-28-2020

Relationships between Willingness to Share Information for Benefits and Trust

Gaurav Bansal
bansalg@uwgb.edu

Fiona Nah

Relationships between Willingness to Share Information for Benefits and Trust

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

Fiona Fui-Hoon Nah
Missouri University of Science and Technology
nahf@mst.edu

ABSTRACT

This research examines the role of willingness to share one's information for three benefits as tradeoffs – monetary gains, personalization, and national security – and their effects on trust in online businesses. Data were gathered from MTurk and the results indicate that willingness to share information for monetary gains and personalization is marginally associated with trust in online businesses, but willingness to share information for national security has no association with trust in online businesses. The paper also discusses implications, limitations, and future research directions.

Keywords

Willingness to share information, monetary benefits, personalization, national security, trust

INTRODUCTION

Privacy is not about being left alone. It is more about an individual's desire to be in control of one's information (Stewart and Segars, 2002). Privacy also relates to the calculus and tradeoff of losses and benefits of sharing one's information (Dinev and Hart, 2006). The cost-benefit analysis associated with the calculus is dependent upon the benefits of sharing information and the costs associated with the anxiety and potential loss of reduced control, as evidenced by unauthorized secondary usage, data breaches, and government snooping, among others (Rainie, 2018). Interestingly while we as a society are concerned about the privacy of our information, we also continue to share even more sensitive and personal data online for personalization (Sheng, Nah and Siau, 2008) and sometimes, for monetary benefits of as little as 25 cents (Grossklags and Acquisti, 2007). People are also known to share information when driven by their desire to enhance perceived self-worth (Wilcox and Stephen, 2013).

Privacy concerns shape how much we trust an entity that is collecting or using our data (Bansal, Zahedi and Gefen, 2010). Perceptions of higher risks are known to lower trust (Bansal et al., 2010; Dinev and Hart, 2006). In the era of the post-Snowden revelation, where there are heightened concerns about government surveillance programs that are built over data collected by private businesses (Geiger, 2018; Rainie, 2016), privacy concerned individuals are wary of trusting businesses. However, willingness to share one's information for a benefit in return (tradeoff) might be associated with increased trust as well. In this paper, we examine the relationship between trust in online businesses and willingness to tradeoff information for (i) monetary gains, (ii) personalization, and (iii) national security.

The paper proceeds as follows: first, we provide the theoretical foundation for the research, then we develop the research model and the hypotheses. Next, we describe the research methodology and data collection. We then present the data analysis and results, and discuss the study's contributions and implications. We conclude the paper by discussing the limitations and future research directions.

THEORETICAL DEVELOPMENT

Based on the privacy-calculus theory, people share or disclose personal information when the benefits are perceived to outweigh the risks of sharing information (Dinev and Hart, 2006). Hence, a risk-benefit tradeoff is carried out before an individual decides whether to disclose personal information. Prior research (see Table 1) shows that users value monetary benefits, personalization, and national security, and are willing to trade off their information under certain circumstances to seek these benefits.

Source	Type of Benefit	Key Findings
Grossklags and Acquisti (2007)	Monetary Benefit	Users are willing to share their information for as little as 25 cents.
Kummer and Schulte (2019)	Monetary Benefit	Cheaper apps use more privacy-sensitive permissions, and users are willing to pay more for apps that require less privacy-sensitive permissions.
Winegar and Sunstein (2019)	Monetary benefit	Customers are willing to pay $5 to maintain data privacy but would demand $80 to allow access to personal data.
Awad and Krishnan (2006)	Personalization	Privacy sensitive consumers are unwilling to participate in personalization as they do not want to be profiled.
Bleier and Eisenbeiss (2015)	Personalization	Privacy intrusive personalized advertisements increase reactance, especially for less trusted retailers.
Chellappa and Shivendu (2010)	Personalization	Privacy concerns moderate the degree of monetary rewards (coupons) and intention to transact with a website.
Sheng et al. (2008)	Personalization	Context moderates the impact of personalization on privacy concerns and adoption intention.
Sutanto, Palme, Tan and Phang (2013)	Personalization	Personalization increases usage only for privacy-safe applications.
Frimpong (2011)	National Security	Travelers support profiling, even if it would invade their privacy in the interest of national security.

Table 1. Literature Review

In this research, we examine how willingness to share information for a tradeoff could impact trust in online businesses. Willingness

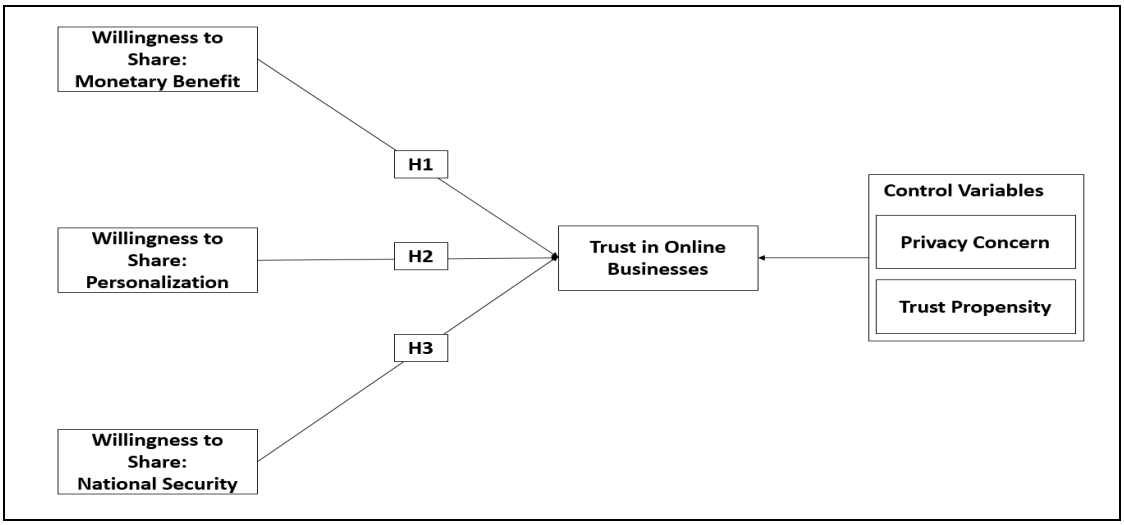

Figure 1. Research Model

to share information in a tradeoff for benefits could generate trust when the trustor believes that the value provided by the tradeoff (i.e., monetary benefit, personalization, and national security) is worthy of sharing one's information, and the trustee

will use one's information appropriately. The trust generated would be low if users believe that the trustee has engaged in prior "psychological contract violation" and has a history of contract violations (e.g., promoting a false advertisement) and misunderstanding about user expectations (Pavlou and Gefen, 2005, p. 372).

We argue that the willingness to share information for tradeoffs in the form of monetary gains, personalization, and national security interest allows individuals to value their information differently, and such valuations inform one's overall privacy concern dynamics (Grossklags and Acquisti, 2007). As a privacy valuation, willingness to share information for tradeoffs (monetary gain, personalization, and national security) would impact trust as well. Willingness to share information for tradeoffs is akin to the (i) personality trait of extroversion, where people are more trusting of others and share their information to receive social energy from such interactions (Zell, McGrath and Vance, 2014), and (ii) personality trait of openness and intellect where individuals analyze their information risks against the gains and take actions to mitigate them as needed (Bansal et al., 2010). While online privacy assurance is associated with positive consumer evaluations, rewards such as financial gains and convenience can significantly increase individuals' desire to transact with a website (Grossklags and Acquisti, 2007). Research on the benefits of personalization (Ozturk, Nusair, Okumus and Singh, 2017) has shown that even though personalization increases privacy concerns for the users, it reduces users' perceived risk and increases their trust towards the website. Similarly, it is found that people are willing to share information for national security reasons (Swire, 2006).

Thus, we have the following three hypotheses:

Hypothesis 1: Willingness to share information for *monetary benefits* is positively associated with trust in online businesses.

Hypothesis 2: Willingness to share information for *personalization* is positively associated with trust in online businesses.

Hypothesis 3: Willingness to share information for *national security* is positively associated with trust in online businesses.

RESEARCH METHODOLOGY

Measurement Development

We used preexisting scales where available, and developed items for various constructs as outlined in Table 2.

Construct	Adapted From
WTS for Monetary Benefits	Self-developed
WTS for Personalization	Self-developed
WTS for National Security	Self-developed
Privacy Concerns	Bansal, Zahedi and Gefen (2015)
Trust Propensity	Bansal and Zahedi (2015)
Trust in Online Businesses	Bélanger and Carter (2008), Teo, Srivastava and Jiang (2008)
Note: WTS – Willingness to share	

Table 2. Measurement Instrument

Research Design and Data Collection

Data was collected from MTurk workers using a Qualtrics survey. Out of 312 people who completed the survey, 275 respondents passed the attention check questions. The final sample of 275 had an average age of 34.4 years (standard deviation of 10 years). The age ranged from 18 to 69 years. There were 155 males and 119 females. One person chose 'other' for gender. 95% of the sample had some college or higher education. 77% were employed full time, 10% were employed part-time, and 10% were self-employed. 89% of them have made purchases online using a credit card, and 82% of them have made purchases using mobile apps.

DATA ANALYSIS

We analyzed the data in two phases. In the first phase, we conducted reliability as well as discriminant and convergent validity analyses and examined the measurement model. The constructs demonstrate adequate reliability, with Cronbach's alpha coefficients of 0.7 and above for all the constructs. Construct correlations are less than the square root of AVE, demonstrating support for discriminant validity. AVE values are greater than .5, demonstrating support for convergent validity. We also found adequate support for discriminant and convergent validity through EFA analysis. The CFA measurement estimates are all significant (p<.001) and greater than 0.7. Also, the fit indices for the CFA model meet the required thresholds, further demonstrating adequate measurement fit (CFI .921, TLI .909, RMSE .058, SRMR .053). The estimation model was then computed in the second phase using Mplus (Muthén and Muthén, 1998-2012). The fit indices for the estimation models are within the suggested thresholds (CFI .921, TLI .909, RMSE .058, SRMR .053), suggesting an adequate estimation-model fit. The results are presented in Figure 2. The model explains 48.1% of the variance in trust in online businesses. The results show that H3 is not supported; however, H1 and H2 are partially supported at p<.10. Path coefficients for control variables suggest that privacy concerns increase trust in online businesses (p<.05). Trust propensity is also positively associated with trust in online businesses at p<.001.

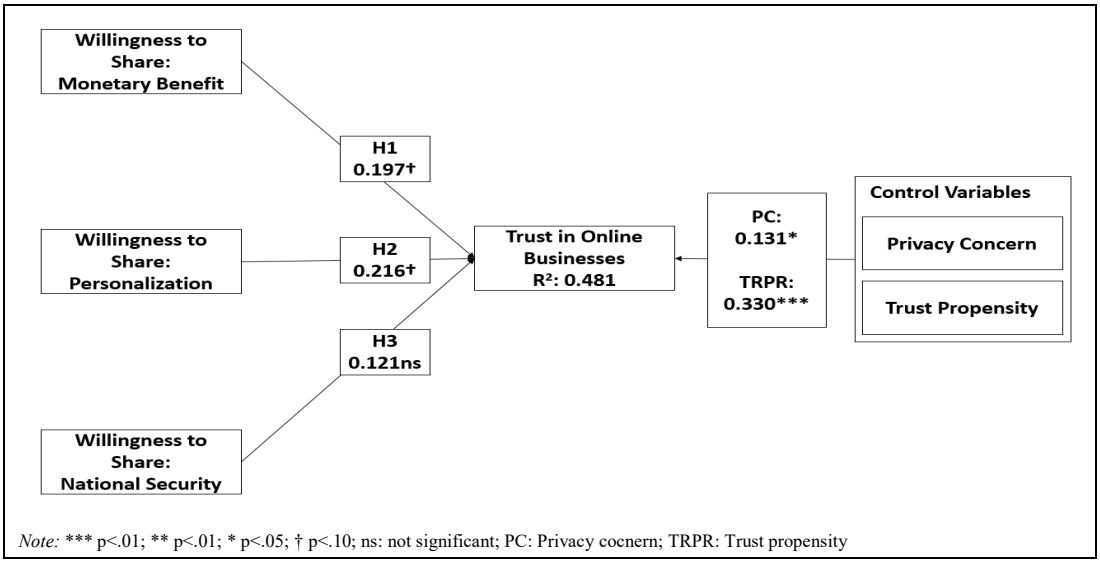

Figure 2. Results

DISCUSSION

Key Findings and Contributions

This paper assesses the relative trust benefits associated with three tradeoffs – monetary benefit, personalization, and national security. Prior research has established that privacy concerns, just like risk beliefs, lower trust in online businesses. There are information asymmetries involved that create opportunities for one to get victimized where one's information could be misused. This risk belief could lower trust in online businesses. However, this research shows that privacy concerns can increase trust when trust propensity is controlled, and the willingness to share one's information for something one values (i.e., personalization and monetary benefit) can enhance trust. Users trust online businesses if they believe that the entity providing the desired trade-off feature (personalization and monetary benefit) will also make the right use of their information. Our results suggest that willingness to share information for monetary gains and through personalization as a non-monetary gain is marginally associated with trust in online businesses after controlling for trust propensity and privacy concerns. However, willingness to share information for national security reasons has no relationship with trust in online businesses. Hence, the relationship between willingness to share information with online businesses and trust is enhanced or increased by monetary gains and personalization but not by national security reasons, which suggests that using national security reasons as a means to collect data from customers is unlikely to influence their trust in online businesses positively. Even though people accept getting screened at airports and do not find it too invasive in the interest of national security (Frimpong, 2011), they are not

trusting online businesses for sharing their information for national security reasons. Perhaps it is the fear of the government or the fear that online businesses are not able to guard their information against indiscriminate government screening adequately.

This study provides several practical implications. It shows that willingness to share information for monetary benefit and personalization has a weak positive impact on trust in online businesses. In contrast, the willingness to share information for national security has no impact on trust in online businesses. Sharing personal information for national security with the government does not enhance user trust. Users do not fully trust online businesses using their data (or perhaps sharing their data with the government) for national security [also see (Nielsen, 2018)]. Hence, users are not willing to trust online businesses as "surveillance intermediaries" (HLR, 2018). This research has suggestions for policymaking when online businesses are increasingly reflecting on their role as surveillance intermediaries (HLR, 2018), as they exhibit reactance turning over their users' data, e.g., Apple vs. FBI (The Washington Post, 2016), and Google vs. NSA (WSJ, 2020). The research also informs online businesses that they can gain users' trust, to some extent, especially when the users are looking for sharing their information for personalization and monetary benefits, but not for national security purposes.

As with any research, it is important to acknowledge the limitations of the study. Future research should test the model with diverse populations and examine the model longitudinally. Future research can look into trust of specific businesses, as well as trust in government surveillance programs. Even though the results show that privacy concerns have a positive relationship with trust in online businesses, which is an interesting finding, it is not surprising given that Bansal et al. (2010) reported that health information privacy concerns did not lower trust in health websites. Future research could look into why privacy concerns could increase trust. Future research could also examine the potential moderating impact of privacy concerns on these tradeoffs and trust relationships, as personalization might lead to lower trust for higher privacy concerned individuals than for low privacy concerned individuals (Chellappa and Shivendu, 2010). It would also be interesting to examine such relationships across different countries since tradeoffs could have different implications in a different culture. For instance, in China, personalization is valued to a greater extent as it makes people perceive themselves to be more highly respected (Xu, 2006).

ACKNOWLEDGEMENT

The research was made possible in part due to Frederick E. Baer Professorship in Business at Austin E. Cofrin School of Business at the University of Wisconsin–Green Bay.

REFERENCES

1. Awad, N. F. and Krishnan, M. D. (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization, *MIS Quarterly* 30, 1, 13-28.
2. Bansal, G., Zahedi, F. and Gefen, D. (2015) The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern, *European Journal of Information Systems* 24, 6, 624-644.
3. Bansal, G. and Zahedi, F. M. (2015) Trust violation and repair: The information privacy perspective, *Decision Support Systems* 71, 62-77.
4. Bansal, G., Zahedi, F. M. and Gefen, D. (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, *Decision Support Systems* 49, 2, 138-150.
5. Bélanger, F. and Carter, L. (2008) Trust and risk in e-government adoption, *The Journal of Strategic Information Systems* 17, 2, 165-176.
6. Bleier, A. and Eisenbeiss, M. (2015) The importance of trust for personalized online advertising, *Journal of Retailing* 91, 3, 390-409.
7. Chellappa, R. K. and Shivendu, S. (2010) Mechanism design for "free" but "no free disposal" services: The economics of personalization under privacy concerns, *Management Science* 56, 10, 1766-1780.
8. Dinev, T. and Hart, P. (2006) An extended privacy calculus model for e-commerce transaction, *Information Systems Research* 17, 1, 61-80.
9. Frimpong, A. (2011) Introduction of full body image scanners at the airports: A delicate balance of protecting privacy and ensuring national security, *Journal of Transportation Security* 4, 3, 221-229.
10. Geiger, A. W. (2018) How Americans have viewed government surveillance and privacy since Snowden leaks, from https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ (last accessed Feb 28, 2020).
11. Grossklags, J. and Acquisti, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information, *Sixth Workshop on the Economics of Information Security (WEIS 2007), Pittsburgh, PA*.

12. HLR. (2018) Cooperation or resistance?: The role of tech companies in government surveillance, *Harvard Law Review*, from https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/ (last accessed Mar 5, 2020).
13. Kummer, M. and Schulte, P. (2019) When private information settles the bill: Money and privacy in Google's market for smartphone applications, *Management Science* 65, 8, 3470.
14. Muthén, L. K. and Muthén, B. O. (1998-2012). *Mplus user's guide (seventh edition)*. Los Angeles, CA: Muthén & Muthén.
15. Nielsen, R. P. (2018) Ethical and legal first amendment implications of FBI v. Apple: A commentary on Etzioni's 'Apple: Good business, poor citizen?', *Journal of Business Ethics* 151, 1, 17-28.
16. Ozturk, A. B., Nusair, K., Okumus, F. and Singh, D. (2017) Understanding mobile hotel booking loyalty: An integration of privacy calculus theory and trust-risk framework, *Information Systems Frontiers* 19, 4, 753-767.
17. Pavlou, P. A. and Gefen, D. (2005) Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role, *Information Systems Research* 16, 4, 372-399.
18. Rainie, L. (2016) The state of privacy in post-Snowden america, from http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (last accessed July 3, 2019).
19. Rainie, L. (2018) Americans' complicated feelings about social media in an era of privacy concerns, from https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns (last accessed Mar 12, 2020).
20. Sheng, H., Nah, F. F.-H. and Siau, K. (2008) An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns, *Journal of the Association for Information Systems* 9, 6, 344-376.
21. Stewart, K. A. and Segars, A. H. (2002) An empirical examination of the concern for information privacy instrument, *Information Systems Research* 13, 1, 36-49.
22. Sutanto, J., Palme, E., Tan, C.-H. and Phang, C. W. (2013) Addressing the personalization–privacy paradox: An empirical assessment from a field experiment on smartphone users, *MIS Quarterly* 37, 4, 1141-1164.
23. Swire, P. P. (2006) Privacy and information sharing in the war on terrorism, *Vill. L. Rev.* 51, 4, 951-980.
24. Teo, T. S., Srivastava, S. C. and Jiang, L. (2008) Trust and electronic government success: An empirical study, *Journal of Management Information Systems* 25, 3, 99-132.
25. The Washington Post. (2016) Apple vows to resist FBI demand to crack iphone linked to san bernardino attacks, from https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html (last accessed Mar 5, 2020).
26. Wilcox, K. and Stephen, A. T. (2013) Are close friends the enemy? Online social networks, self-esteem, and self-control, *Journal of Consumer Research* 40, 1, 90-103.
27. Winegar, A. G. and Sunstein, C. R. (2019) How much is data privacy worth? A preliminary investigation, *Journal of Consumer Policy* 42, 3, 425-440.
28. WSJ. (2020) Google resists demands from states in digital-ad probe from https://www.wsj.com/articles/google-resists-demand-from-states-in-digital-ad-probe-11582281000 (last accessed Mar 5, 2020).
29. Xu, D. J. (2006) The influence of personalization in affecting consumer attitudes toward mobile advertising in china, *Journal of Computer Information Systems* 47, 2, 9-19.
30. Zell, D., McGrath, C. and Vance, C. M. (2014) Examining the interaction of extroversion and network structure in the formation of effective informal support networks, *Journal of Behavioral and Applied Management* 15, 2, 59-81.